CLAIMS

1. A credential communication device adapted to transmit and receive data, including means to process said data in order to effect credential verification and trusted mutual recognition between the device and a second credential communication device, without reference to a third party, further including at least one proximity conductor adapted to transfer at least some data only when in such physical proximity to a second credential communication device as to effectively exclude the possibility of third party involvement in the transaction.

2. A credential communication device as in claim 1, further adapted to require a user of the device to authenticate their identity immediately before communication with the second device.

3. A credential communication device as in claim 1or claim 2 further adapted to accept identity authentication by the keying of a pass code into the device.

4. A credential communication device as in claim 1or claim 2 further adapted to accept identity authentication by use of a biometric authentication apparatus.

5. A credential communication device as in any one of the preceding claims wherein the proximity connector is an induction connection.

6. A credential communication device as in claim 5, wherein the induction connection is effected by a RF transceiver of such power as to require the physical proximity to be such as approximates physical touch.

7. A credential communication device as in any one of the preceding claims wherein there are means to effect variation in the power output of the proximity conductor in relation to the data to be transmitted wherein in use selected data, which is data whose unauthorised reception is acceptable, is transmitted at such power as to be received by the second device before said physical proximity to the second device as to effectively exclude the possibility of third party involvement in the transaction is established, and other selected data, which is data whose unauthorised reception is not acceptable, is transmitted at such a power as to be received only when the credential exchange device is in such

physical proximity to a second credential exchange device as to effectively exclude the possibility of third party involvement in the transaction.

8. A credential communication device as in any one of the preceding claims wherein the proximity conductor includes means to detect that physical touch is being maintained between the device and a second device, the device further adapted to transfer some data only when such touch is detected.

9. A credential communication device as in claim 8 wherein the means to detect physical touch is a pressure sensor.

10. A credential communication device as in any one of the preceding claims wherein the proximity connector is protected from physical or environmental damage by a thin layer or shell of material.

11. A credential communication device as in any one of the preceding claims including means to communicate the results of processing to effect credential verification.

12. A credential communication device as in claim 11 wherein said communication means includes at least one trusted light indicator.

13. A credential communication device as in claim 11 wherein said communication means includes at least three separately identifiable trusted light indicators.

14. A credential communication device as in any one of claims 11-13 wherein said light indicators are formed as bands around the device to facilitate visibility from multiple angles.

15. A credential communication device as in any one of claims 11-14 wherein said light indicators are light emitting diodes.

16. A credential communication device as in any one of the preceding claims further including a trusted alpha-numeric display.

17. A credential communication device as in any one of the preceding claims further including a biometric authentication apparatus.

18. A credential communication device as in claim 17 wherein said biometric authentication apparatus is a fingerprint scanner.

19. A credential communication device as in any one of the preceding claims further including means for receiving wireless transmissions from a distance further than the range of the proximity conductor.

20. A credential communication device as in any one of the preceding claims wherein the device is approximately cylindrical.

21. A credential communication device as in claim 20 wherein the proximity conductor is located on the shaft of said approximately cylindrical structure, permitting momentary contact with a second device from a variety of angles.

22. A credential communication device as in any one of the preceding claims wherein the proximity conductor is a bulbous structure, permitting momentary contact with a second device from a variety of angles.

23. A credential communication device as in any one of the preceding claims wherein the device is a component in a mutually authenticated ensemble of devices, the device being adapted to effect data display on a trusted remote visual display device.

24. A credential communication device as in claim 23 wherein the remote visual display device is a badge display.

25. A set of devices where a first of the devices is adapted to hold information in an electronic storage and effect transmission of such information upon a triggering of such transmission, and a second device is adapted to hold data in an electronic storage and adapted to receive transmissions from said first device and effect a comparison of such received data with that being held by said second device and when such received data is matching preselected criteria effect an output signal to this effect, the respective devices being adapted to effect a transmission and receiving between the devices only when in a selected range of distance apart or when touching.

26. A set of devices as in claim 25 wherein said devices are adapted to effect credential accreditation information.

27. A set of devices as in claim 26, wherein the devices have a range of transmission and reception such that they will transmit and receive at least some

data only when in such physical proximity as to effectively exclude the possibility of third party involvement in the transaction.

28. A method for mutual suspicion credential exchange including the steps of:
positioning a credential exchange device as in any one of claims 1-24 to touch or come into close proximity with a second such device,
the credential exchange device transmitting data to and receiving data from the second device,
the credential exchange device processing received data to determine the credential status of the second device,
the credential exchange device outputting the results of the credential determination.

29. A method for mutual suspicion credential exchange including the steps of:
providing each participant with a credential exchange device as in any one of claims 1-24,
loading the credential exchange device with credential data relevant to a user,
each participant operating their device to seek appropriate credential data from a second device,
each participant positioning their device to touch or come into close proximity with a second device,
each device transmitting data to and receiving data from a second device,
each device processing received data to determine the credential status of the second device,
each device outputting the results of the credential determination.

30. A method as in any one of claims 28-29 further including the steps of communicating an organisational mandatory security policy to the credential exchange device, and the device applying said mandatory security policy to the data transmitted to the second device.

31. The method of claim 30 wherein the communication of the organisational mandatory security policy is restricted to being a one-off process performed when the device is manufactured or first activated.

32. The method of any one of claims 28-31 further including the steps of communicating a user discretionary security policy to the credential exchange

device, and the device applying said user discretionary security policy to the data transmitted to the second device.

33. The method of claim 32 wherein the communication of the user discretionary security policy is restricted to being a one-off process performed when the device is manufactured or first activated.

34. The method of claim 30 wherein the mandatory security policy is communicated to the credential communication device by means localised to the particular location in which the device is operating.

35. The method of claim 34 wherein said policy communication is by secure wireless means.

36. The method of any one of claims 28-35 including the step of the credential communication device signalling via secure wireless means to a remote visual display means in its own ensemble a visual depiction of the participant associated with the second device.

37. A method for rapid verification of the credentials of a group of participants by a guard including the steps of:
providing each participant and the guard with a credential communication device as in any one of claims 1-24,
loading each participant's credential communication devices with data including the identity and credentials of the participant,
operating the guard's device to cause it to seek appropriate identity or credential data from a participant's device,
positioning each participant's device to touch or come into close proximity with the guard's device,
transmitting data and receiving data between the guard's and the participant's devices,
the guard's device processing received data to determine the credential status of the participant's device,
the guard's device outputting the results of the credential determination.

38. The method of claim 37 further including the step of providing a passive device adapted to extend the area in which proximity to the guard's device is sufficient for the proximity conductor to operate.

39. The method of claim 38 wherein the passive device is a waveguide, adapted to allow the guard's credential communication to be inserted into it, further including the step of each participant passing their credential communication device through the waveguide to communicate their credentials.

40. The method of any one of claims 37-39 wherein the guard's device is a component in an ensemble including a remote visual display device and further including the step of the guard's credential communication device signalling via secure wireless means to the remote visual display means in its own ensemble a visual depiction of the participant associated with the participant's device.

41. A portable tamper resistant trusted device adapted to be used for personal identification, credential warrants, and credential exchange including an inductive connector, one or more trusted input switches, one or more trusted light displays to permit viewing from multiple angles, a trusted display, an untrusted wheel press button, an untrusted audio generator, and a wireless network interface.

42. A device as in claim 41wherein the display is untrusted.

43. A credential communication device substantially as described with respect to any one of the embodiments in the specification with reference to and as illustrated by the accompanying illustrations with respect to that embodiment.

44. A method for mutual suspicion credential exchange substantially as described with respect to any one of the embodiments in the specification with reference to and as illustrated by the accompanying illustrations with respect to that embodiment.